

Universal test for Hippocratic randomness

Hayato Takahashi*

December 23, 2014

Abstract

Hippocratic randomness is defined in a similar way to Martin-Löf randomness, however it does not assume computability of the probability and the existence of universal test is not assured. We introduce the notion of approximation of probability and show the existence of the universal test (Levin-Schnorr theorem) for Hippocratic randomness when the logarithm of the probability is approximated within additive constant.

Keywords: Hippocratic randomness, blind randomness, Kolmogorov complexity, universal test

1 Introduction

In [1, 2], the notion of Hippocratic (blind) randomness is introduced. Hippocratic randomness is defined in a similar way to Martin-Löf randomness, however it does not assume computability of the probability. On the other hand if we do not assume computability of the probability, the existence of universal test is not assured. In this paper, we introduce the notion of approximation of probability and show the existence of the universal test (Levin-Schnorr theorem) for Hippocratic randomness when the logarithm of the probability is approximated within additive constant.

Let Ω be the set of infinite binary sequences and S be the set of finite binary strings, respectively. Let $\Delta(s) := \{sx^\infty | x^\infty \in \Omega\}$ for $s \in S$, where sx^∞ is the concatenation of s and x^∞ . In the following, we study probabilities on (Ω, \mathcal{B}) , where \mathcal{B} is the Borel- σ -algebra generated from $\Delta(s)$, $s \in S$, and we omit \mathcal{B} if it is obvious from the context. For a probability P on Ω , we write $P(s) := P(\Delta(s))$ for $s \in S$.

*1-1 Yanagido, Gifu City 501-1193, Japan. Organization for Promotion of Higher Education and Student Support, Gifu University. hayato.takahashi@ieee.org

For $A \subseteq S$, let $\tilde{A} := \cup_{s \in A} \Delta(s)$. An r.e. set $U \subseteq \mathbb{N} \times S$ is called test w.r.t. P if $U_n \supseteq U_{n+1}$ and $P(\tilde{U}_n) < 2^{-n}$, where $U_n := \{x \mid (n, x) \in U\}$, for all n . The set of Hippocratic random sequences w.r.t. P (in the following we denote it by \mathcal{H}^P) is the set that is not covered by any limit of test, i.e., $\mathcal{H}^P := (\cup_{U: \text{blind test}} \cap_n \tilde{U}_n)^c$. In this definition, we can replace $P(\tilde{U}_n) < 2^{-n}$ with $P(\tilde{U}_n) < f(n)$, where f is a computable decreasing function. If P is computable, \mathcal{H}^P is equivalent to Martin-Löf (ML-)randomness (in the following we denote it by \mathcal{R}^P).

Next we introduce a notion of approximation. We say that a probability P on Ω is *log-approximative* if there is a computable $f : S \rightarrow \mathbb{N}$ such that

$$\exists c \forall x \ f(x) < -\log P(x) < f(x) + c. \quad (1)$$

Throughout the paper, the base of logarithm is 2. For more details of the notion of approximation, see [8]. We can construct an example of probability on Ω that is log-approximative but not computable in a similar manner to the example (Theorem 2.4) in [8].

In the following, $A \subset S$ is called prefix-free (non-overlapping) if $\Delta(x) \cap \Delta(y) = \emptyset$ for all $x, y \in A, x \neq y$. We see that if A is r.e. then there is a prefix-free r.e. set A' such that $\tilde{A} = \tilde{A}'$. Let K_m be the 1-dimensional monotone complexity, see [3, 4, 9]. For a prefix-free set A we have $\sum_{x \in A} 2^{-K_m(x)} \leq 1$, see [7]. The following theorem shows that Levin-Schnorr theorem [3, 5, 6] holds for Hippocratic randomness if the probability is log-approximative.

Theorem 1.1 (Levin-Schnorr theorem for Hippocratic randomness)

Let P be a log-approximative probability on Ω . Then

$$x^\infty \in \mathcal{H}^P \Leftrightarrow \sup_{x \sqsubset x^\infty} -\log P(x) - Km(x) < \infty.$$

Proof) Suppose that $x^\infty \notin \mathcal{H}^P$. Then there is a test U such that $x^\infty \in \tilde{U}_n$ and $P(\tilde{U}_n) < 2^{-n}$ for all n . Then there is an r.e. set U' such that $\tilde{U} = \tilde{U}'_n$ and U'_n is prefix-free for all n , where $U'_n := \{x \mid (n, x) \in U'\}$. Let $P'(x) = P(x)2^n$ for $x \in U'_n$ and 0 otherwise. From (1), we have

$$\sum_{x \in U'_n} 2^{-(f(x)+c)+n} \leq \sum_{x \in U'_n} P'(x) \leq 1.$$

Let $P''(x) := 2^{-(f(x)+c)+n}$ for $x \in U'_n$ and 0 otherwise. Since f is computable and $x^\infty \in \cap_n \tilde{U}'_n$, by applying Shannon-Fano-Elias coding to P'' , we have

$$\begin{aligned} \exists c_1, c_2 \forall n \exists x \sqsubset x^\infty \quad Km(x) &\leq f(x) - n + 2 \log n + c_1 \\ &\leq -\log P(x) - n + 2 \log n + c_2, \end{aligned}$$

where the last inequality follows from (1).

Conversely, let

$$\forall n \ U_n := \{x \mid Km(x) < -\log P(x) - n\} \text{ and } V_n := \{x \mid Km(x) < f(x) - n\}.$$

From (1), we have

$$\exists c \forall n \ V_n \subseteq U_n \subseteq V_{n-c}.$$

Since f is computable, $\{V_n\}_{n \in \mathbb{N}}$ is uniformly r.e., and

$$\forall n \ P(\tilde{V}_n) \leq P(\tilde{U}_n) \leq \sum_{x \in U'_n} 2^{-Km(x)-n} \leq 2^{-n},$$

where U'_n is a prefix-free set such that $\tilde{U}'_n = \tilde{U}_n$. Therefore $\{V_n\}_{n \in \mathbb{N}}$ is a test. Since $\cap_n \tilde{V}_n = \cap_n \tilde{U}_n$, we have the theorem. \blacksquare

Acknowledgement

This work is supported by JSPS KAKENHI Grant number 24540153.

References

- [1] L. Bienvenu, P. Gacs, M. Hoyrup, C. Rojas, and A. Shen. Algorithmic tests and randomness with respect to a class of measures, 2011. arXiv:1103.1529v2.
- [2] Bjørn Kjos Hanssen. The probability distribution as a computational resource for randomness testing. *Journal of Logic and Analysis*, 2(10):1–13, 2010.
- [3] L. A. Levin. On the notion of a random sequence. *Soviet. Math. Dokl.*, 14(5):1413–1416, 1973.
- [4] M. Li and P. Vitányi. *An introduction to Kolmogorov complexity and Its applications*. Springer, New York, third edition, 2008.
- [5] C. P. Schnorr. Process complexity and effective random tests. *J. Comp. Sys. Sci.*, 7:376–388, 1973.
- [6] C. P. Schnorr. A survey of the theory of random sequences. In Butts and Hintikka, editors, *Basic problems in Methodology and Linguistics*, pages 193–211. Reidel, Dordrecht, 1977.
- [7] H. Takahashi. Algorithmic randomness and monotone complexity on product space. *Inform. and Compt.*, 209:183–197, 2011.
- [8] H. Takahashi. Generalization of van Lambalgen’s theorem and blind randomness for conditional probabilities, 2014. arXiv:1310.0709v3.
- [9] V. A. Uspenskii, A. L. Semenov, and A. Kh. Shen. Can an individual sequence of zeros and ones be random? *Russian Math. Surveys*, 45(1):121–189, 1990.